S3 1 PN=EP 77238

3/5/1
DIALOG(R)File 351:Derwent WPI

003607258
WPI Acc No: 1983-F5456K/*198317*
XRPX Acc No: N83-072196
Validation system for signature on transmitted message - uses memory at receiver to recover signature from secret coded transmitted information
Patent Assignee: CII-HONEYWELL BULL (SELA)
Inventor: MOLLIER J; SAADA C
Number of Countries: 009 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 77238	A	19830420	EP 82401752	A	19820928	198317 B
FR 2514593	A	19830415				198320
EP 77238	B	19860205				198606
DE 3268974	G	19860320				198613
US 4656474	A	19870407	US 85799300	A	19851120	198716

Priority Applications (No Type Date): FR 8119090 A 19811009
Cited Patents: EP 21401; EP 35448; 1.Jnl.Ref
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 77238	A	F	24		
Designated States (Regional): CH DE FR GB IT LI NL SE					
EP 77238	B	F			
Designated States (Regional): CH DE FR GB IT LI NL SE					

Abstract (Basic): EP 77238 A

A transmission unit comprises a keyboard coupled to a memory with an inaccessible section containing the secret code for a person while the accessible section contains a computer program for a signature. A processor processes the program and accepts message data from the keyboard to pass the results to circuits to combine the message and signature. The message is coded for transmission to a receiver via a transmission line.

The message is received by circuits which reconstitute it into its original form for display on a VDU. An I/O interface permits printing of the message on paper. A processor accesses data in a memory and authenticates the signature by computing the secret key of the transmitter of the message from data prerecorded in a control card. A

circuit compares the two signatures to issue a validation signal for an indicator.

Title Terms: VALID; SYSTEM; SIGNATURE; TRANSMIT; MESSAGE; MEMORY; RECEIVE; RECOVER; SIGNATURE; SECRET; CODE; TRANSMIT; INFORMATION

Derwent Class: W01

International Patent Class (Additional): G06K-005/00; H04L-009/00; H04Q-009/00

File Segment: EPI

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication: **0 077 238**
A1

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt: **82401752.9**

(51) Int. Cl.³: **H 04 L 9/00**

(22) Date de dépôt: **28.09.82**

(30) Priorité: **09.10.81 FR 8119090**

(43) Date de publication de la demande: **20.04.83**
Bulletin 83/16

(84) Etats contractants désignés: **CH DE FR GB IT LI NL SE**

(71) Demandeur: **COMPAGNIE INTERNATIONALE POUR L'INFORMATIQUE CII - HONEYWELL BULL (dite CII-HB), 94, avenue Gambetta, F-75020 Paris (FR)**

(72) Inventeur: **Moller, Jean, 94 avenue Gambetta, F-75020 Paris (FR)**
Inventeur: **Saada, Charles, 94 avenue Gambetta, F-75020 Paris (FR)**

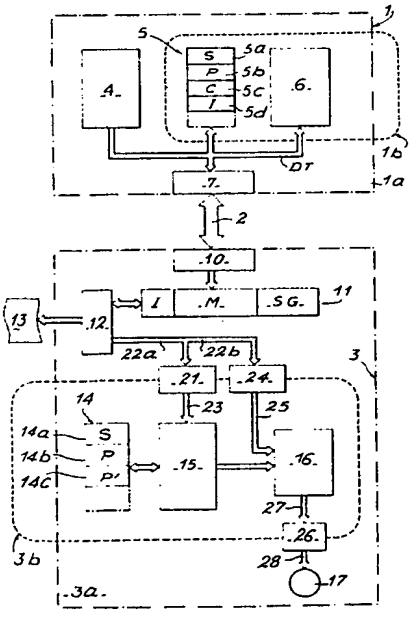
(74) Mandataire: **Doireau, Marc et al, 94, avenue Gambetta, F-75020 Paris (FR)**

(54) Procédé et dispositif pour authentifier la signature d'un message signé.

(57) L'invention a pour objet un procédé et un dispositif pour authentifier la signature d'un message signé.

Selon l'invention, une carte de signature nominative (1a) est accouplable à un appareil émetteur 1 de transmission de messages signés. La carte (1a) comprend au moins une mémoire (5) où sont au moins pré-enregistrés, de façon secrète, une clé secrète (S) et un programme (P) d'élaboration automatique de la signature d'un message (M) et des circuits de calcul (6) de la signature (SG). Une carte de contrôle (3b), non nominative, est accouplable à un appareil récepteur (3) de messages signés. La carte (3b) comprend au moins une mémoire où sont au moins pré-enregistrés, de façon secrète, la clé secrète (S) et le programme (P) pour recalculer, par des circuits de traitement (15), la signature (SG) du message (M) reçu.

L'invention s'applique notamment à la transmission de données.



EP 0 077 238 A1

0077238

PROCEDE ET DISPOSITIF POUR AUTHENTIFIER LA SIGNATURE D'UN MESSAGE SIGNE

L'invention concerne généralement et a essentiellement pour objet un procédé et un dispositif pour authentifier la signature d'un message signé reçu par un appareil récepteur et transmis à partir d'un appareil émetteur par une voie de transmission quelconque.

D'une façon générale, un message est signé dès l'instant où l'on associe à ce message la signature de l'émetteur de ce message. Pour une meilleure compréhension de l'invention, il est important de définir au préalable ce qu'il faut entendre concrètement par message et par signature :

- message : un message est constitué par toute suite de caractères alphanumériques représentatifs d'un texte en clair ou d'un texte codé, cette suite pouvant être avantageusement remplacée par une représentation contractée en utilisant par exemple les codes de Hamming.

- signature : une signature est constituée par toute suite de caractères alphanumériques représentatifs de l'identité de l'émetteur du message qui peut être indifféremment une personne physique ou morale.

Associer une signature à un message n'est en fait, dans la majorité des cas, qu'une simple juxtaposition du contenu du message et de la signature de l'émetteur du message. En effet, signer un message ne revient qu'à accoler au message une signature avec généralement interposition d'un signe de ponctuation.

Il devient alors compréhensible qu'une telle juxtaposition laisse la possibilité à un fraudeur de combiner à volonté des messages et des signatures d'origines différentes.

Pour pallier cet inconvénient majeur ou l'absence de lien réel entre un message et sa signature, la demanderesse a décrit, dans sa demande de brevet français n° 80 07 912 déposée le 9 avril 1980 et non encore publiée, un système de transmission qui lie de façon automatique et indissociable le contenu ou texte d'un message à sa signature. Ainsi, à chaque message du même signataire correspond une signature différente et deux messages identiques émis par des personnes différentes n'ont pas la même signature. L'élaboration d'une telle signature fait essentiellement appel à un programme de calcul de signature qui prend en compte non seulement le contenu du message, mais également au moins un paramètre dénommé clé secrète inconnue même de l'émetteur du message.

S'il est ainsi permis de limiter les risques de fraude, l'authentification de la signature d'un message devient plus complexe étant donné qu'à tout message d'un même émetteur est associée une signature différente.

L'objet de la présente invention est justement de concevoir un procédé qui permette d'authentifier, d'une façon simple, la signature d'un message élaborée automatiquement comme décrit dans la demande de brevet précitée, sans pour autant donner à une quelconque personne les moyens lui permettant de prendre connaissance de la signature réelle d'un message dont la signature aurait été volontairement ou involontairement modifiée.

L'invention a donc pour objet un procédé pour authentifier la signature d'un message signé reçu par un appareil récepteur et transmis à partir d'un appareil émetteur par une voie de transmission quelconque, la signature d'un message étant élaborée automatiquement au niveau de l'appareil émetteur à partir d'un programme de calcul de signature faisant au moins appel au contenu du message à

transmettre et à un paramètre ou clé secrète inconnue de l'émetteur du message, caractérisé en ce qu'il consiste, pour vérifier l'authenticité de la signature d'un message reçu par l'appareil récepteur :

- à recalculer automatiquement la signature du message reçu à partir d'au moins le même programme de calcul de signature précité prenant en compte le contenu du message reçu et la même clé secrète précitée également inconnue du récepteur du message,

- à comparer automatiquement la signature du message reçu et la signature recalculée par l'appareil récepteur,

- et à indiquer seulement au récepteur du message, le résultat égal ou différent de la comparaison précédente tout en interdisant au récepteur du message la possibilité de pouvoir prendre connaissance de la valeur de la signature recalculée.

Toutefois, bien qu'inconnue de la personne émettrice d'un message, la clé secrète précitée n'en est pas moins attribuée à cette personne et à cette seule personne. Aussi, si l'appareil récepteur ne prend en compte qu'une seule clé secrète, il ne pourra alors authentifier que des signatures de messages signés émis par la seule et unique personne à laquelle cette clé secrète a été attribuée.

Pour lever cette limitation, le procédé conforme à l'invention prévoit en plus, au niveau de l'appareil récepteur, la possibilité d'authentifier des messages signés émis par des personnes différentes.

Aussi, selon une autre caractéristique importante de l'invention, le procédé consiste :

- au niveau de l'appareil émetteur : à autoriser plusieurs personnes à émettre des messages signés avec élaboration automatique de la signature, chaque personne ayant d'une part, une clé secrète propre inconnue de la personne, et d'autre part une identité non secrète transmise avec le message, et

- au niveau de l'appareil récepteur : avant de recalculer la signature du message reçu, à déterminer automatiquement la clé secrète de l'émetteur du message à partir de l'identité de l'émetteur transmise avec le message.

Ainsi, l'identité d'un signataire d'un message est définie :

- explicitement par son identité qu'il communique au destinataire, et

- implicitement par l'usage d'une clé secrète utilisée lors de l'élaboration de la signature.

Il y a donc un couple (identité-clé secrète) qui ne peut être dissocié.

Selon une autre caractéristique importante de l'invention, le procédé consiste à subdiviser la clé secrète de chaque personne émettrice d'un message en n clés élémentaires secrètes choisies parmi m clés élémentaires secrètes regroupées dans une zone mémoire secrète de l'appareil récepteur, et à identifier chaque personne émettrice par n paramètres représentatifs des adresses de n clés élémentaires dans la zone mémoire secrète précitée, ces n paramètres étant transmis avec le message pour permettre à l'appareil récepteur de calculer automatique-ment et secrètement, au moyen d'un programme par exemple, la clé

secrète de la personne émettrice avant de recalculer la signature du message reçu.

L'invention concerne également un dispositif pour la mise en oeuvre du procédé tel que défini précédemment, du type consitité par un appareil émetteur relié par une voie de transmission quelconque à un appareil récepteur, appareil émetteur comprenant au moins un dispositif de mémorisation dans lequel sont au moins enregistrés un programme de calcul de signature et un paramètre ou clé secrète inconnue de l'émetteur du message ; un circuit de traitement pour élaborer automatiquement la signature d'un message à partir du programme de calcul précité prenant en compte le contenu du message et la clé secrète précitée, caractérisé en ce que l'appareil récepteur comprend au moins :

- un dispositif de mémorisation dans lequel sont au moins enregistrés le programme de calcul précité et la même clé secrète précitée également inconnue du récepteur du message,

- des circuits de traitement pour recalculer la signature d'un message reçu à partir du contenu du message, du programme et de la clé secrète,

- un dispositif de comparaison dont une première entrée reçoit de l'extérieur la signature du message reçu et dont la seconde entrée reçoit la signature recalculée par les circuits de traitement précités, et

- un dispositif témoin à au moins deux états stables indiquant respectivement les résultats vrai ou différent de la comparaison précitée, l'entrée du dispositif témoin étant reliée à la sortie du dispositif de comparaison précité.

Selon une autre caractéristique importante du dispositif conforme à l'invention, le dispositif de mémorisation de l'appareil récepteur contient une première zone secrète dans laquelle sont pré-enregistrés les m clés élémentaires précitées, et une deuxième zone dans laquelle est pré-enregistré un second programme ou programme de calcul de la clé secrète de la personne émettrice d'un message à partir des n paramètres précités représentatifs des adresses des n clés élémentaires et transmis avec le message.

Selon une autre caractéristique importante de l'invention :

- l'appareil émetteur est composé de deux parties : une partie fixe accessible à toute personne qui est destinée à assurer la transmission d'un message, et un dispositif portatif dénommé carte de signature personnelle à chaque personne et renfermant de façon inaccessible depuis l'extérieur la clé secrète de la personnne, les circuits de traitement pour calculer la signature d'un message à partir du contenu du message et de la clé secrète, et de préférence le programme d'élaboration automatique de cette signature, et

- l'appareil récepteur est composé de deux parties : une partie fixe accessible à toute personne susceptible de recevoir un message, et un dispositif portatif dénommé carte de contrôle à la disposition de plusieurs personnes et renfermant, de façon inaccessible depuis l'extérieur, le dispositif de mémorisation précité, les circuits de traitement et le circuit de comparaison.

D'autres caractéristiques, avantages et détails ressortiront de l'explication qui va suivre en se reportant à la figure annexée qui représente

schématiquement sous forme de schéma-bloc un mode de réalisation préférentiel de l'invention.

Le problème posé et résolu par l'invention consiste à authentifier à la réception la signature d'un message signé transmis par une voie de transmission quelconque.

Soit un appareil émetteur (1), du type de celui décrit dans la demande de brevet français précitée, et qu'il n'est pas nécesaire de redécrire en détail. Cet appareil émetteur (1), mis à la disposition d'au moins un émetteur personne physique ou représentative d'une personne morale, est relié par une voie de transmission quelconque telle que figurée en (2) à un appareil de réception (3) mis à la disposition d'au moins un récepteur personne physique ou représentative d'une personne morale.

Pour la compréhension de l'invention, il suffit de savoir que l'appareil émetteur (1) comprend au moins :

- un dispositif de saisie de données (4) tel qu'un clavier de machine à écrire d'une machine de traitement de texte par exemple, destiné à prendre en compte un message M à transmettre et éventuellement capable de le transformer en un message contracté représentatif (utilisation des codes Hamming par exemple),

- un dispositif de mémorisation (5) ou mémoire qui comprend au moins deux zones (5a) et (5b), la zone (5a) étant inacessible depuis l'extérieur et renfermant la clé secrète S d'une personne, la zone (5b) renfermant un programme de calcul P de signature SG,

- des circuits de traitement (6) pour dérouler le programme P de calcul de signature, reliés d'une part à la mémoire (5) et d'autre part au dispositif de saisie de données (4),

- un ensemble de circuits (7) reliés d'une part aux circuits de traitement (6) et d'autre part au dispositif de saisie de données (4), pour associer le contenu du message M à sa signature SG calculée par les circuits de traitement (6), pour chiffrer éventuellement le message M afin de le rendre incompréhensible à toute personne, et pour assurer sa transmission par la voie de transmission (2) vers l'appareil récepteur (3).

L'ensemble des liaisons entre les différents éléments précédents est schématisé par un bus de liaison DT.

De façon avantageuse, l'appareil émetteur (1) est constitué en deux parties :

- un dispositif fixe (1a) accessible à toute personne et destiné à assurer la transmission d'un message avec élaboration automatique ou non de la signature,

- un dispositif portatif (1b) ou carte de signature personnelle à chaque personne renfermant de façon inaccessible depuis l'extérieur la clé secrète attribuée nominativement à une personne et inconnue de cette personne, le dispositif de mémorisation (5) et les circuits de traitement (6).

L'appareil récepteur (3) comprend au moins :

- un ensemble de circuits (10) qui reçoivent le message M signé et destinés à restituer le message sous sa forme d'origine en fonction de son mode de transmission déterminé par l'ensemble des circuits (7) de l'appareil émetteur (1),

- un dispositif de visualisation (11) relié aux circuits (10) pour afficher en clair le message signé d'origine ;

ce dispositif de visualisation (11) étant avantageusement relié à un dispositif d'entrée/sortie (12) permettant notamment d'imprimer le message signé reçu sur un support papier (13) par exemple,

- un dispositif de mémorisation (14) ou mémoire qui comprend au moins trois zones (14a), (14b) et (14c) dans lesquelles sont respectivement pré-enregistrés : m clés élémentaires secrètes, le programme de calcul P de signature SG précité, et un second programme P' de calcul de la clé secrète de la personne qui a émis un message,

- des circuits de traitement (15) reliés d'une part à la mémoire (14) et d'autre part au dispositif d'entrée/sortie (12), ces circuits de traitement ayant accès aux informations enregistrées dans la mémoire (14),

- un circuit de comparaison (16) dont une entrée est reliée à la sortie des circuits de traitement (15) et dont l'autre reliée au dispositif d'entrée/sortie (12) et

- un circuit témoin (17) à deux états stables, telle qu'une lampe, dont l'entrée est reliée à la sortie du circuit comparateur (16).

Selon une caractéristique importante de l'invention, la zone (14a) de la mémoire (14), les circuits de traitement (15) et le comparateur (16) doivent être inaccessibles depuis l'extérieur pour éviter à tout tiers de pouvoir prendre connaissance des informations enregistrées et traitées par ces circuits. De préférence, les programmes P et P' sont également rendus inaccessibles depuis l'extérieur.

De façon avantageuse, l'appareil récepteur (3) est constitué en deux parties :

- une partie fixe (3a) comprenant l'ensemble de circuits (10), le dispositif de visualisation (11), le dispositif d'entrée-sortie (12) et le circuit témoin (17),

- une seconde partie portative (3b) dénommée carte de contrôle accessible à plusieurs personnes et renfermant, de façon inaccessible depuis l'extérieur, le dispositif de mémorisation (14), les circuits de traitement (15) et le circuit de comparaison (16).

La carte de signature (1b) et la carte de contrôle (3b) sont conçues et organisées selon les techniques décrites par les brevets français de la Demanderesse n° 2 337 381 et n° 2 401 459.

Dans une telle réalisation, la carte de contrôle (3b) est accouplable au dispositif récepteur (3) et seules certaines entrées-sorties de cette carte (3b) sont accessibles depuis l'extérieur. Plus précisemment en se reportant à la figure 1, cette carte (3b) comprend des premières bornes d'entrée (21) reliées d'une part par des liaisons (22a) au dispositif d'entrée-sortie (12) et d'autre part par des liaisons (23) aux circuits de traitement (15) ; des secondes bornes d'entrée (24) reliées d'une part au dispositif d'entrée-sortie (12) par des liaisons (22b) et d'autre part à une borne d'entrée du comparateur (16) par des liaisons (25) ; et des troisièmes bornes de sortie (26) reliées d'une part par des liaisons (27) à la sortie du circuit de comparaison (16) et d'autre part à l'élément témoin (17) par des liaisons (28).

Pour rendre la carte de signature (1b) nominative, il est important de la personnaliser par un code confidentiel C connu de la personne à laquelle est attribuée cette carte. Aussi, il est nécessaire de prévoir au moins une troisième zone (5c) dans la mémoire (5) de la carte de signature

(1b) dans laquelle est enregistré le code confidentiel C. Cette mesure permet d'éviter l'utilisation de la carte de signature (1b) par une autre personne que celle à laquelle cette carte a été attribuée.

Il va être maintenant décrit le fonctionnement de l'ensemble tel que défini précedemment.

Soit une personne dénommée émetteur désireux de transmettre un message M à une autre personne dénommée récepteur.

Dans une première phase, l'émetteur élabore son message, sa contraction éventuelle, au niveau du dispositif de saisie de données (4) du dispositif émetteur (1). L'émetteur associe à son message une identification I propre à cet émetteur et avantageusement constituée de n paramètres représentatifs des adresses de n clés élémentaires parmi les m élémentaires enregistrées dans la zone secrète (14c) de la mémoire (14). Il peut être avantageux d'associer automatiquement l'identification I de l'émetteur au message qu'il désire transmettre. Pour cela, il suffit de prévoir une zone (5c) dans la mémoire (5) où est pré-enregistrée l'identification I de l'émetteur, c'est-à-dire les n paramètres précités.

Si l'émetteur désire signer son message avant de le transmettre, il doit insérer sa carte nominative de signature (1b) dans la partie fixe (1a) de l'appareil émetteur (1). Une fois cet accouplement effectué, l'émetteur frappe son code confidentiel C au niveau du dispositif de saisie des données (4). Ce code confidentiel C est comparé automatiquement avec le code confidentiel C préalablement enregistré dans la zone (5c) de la mémoire (5) de la carte de signature (1b). Si il y a identité entre les deux codes la carte de signature (1b) est

validée au niveau de l'appareil émetteur (1) et le processus de transmmission d'un message signé est alors initialisé.

Dans une seconde phase, le dispositif émetteur (1) élabore automatiquement la signature SG du message M. Cette élaboration s'effectue soit à partir du message proprement dit, soit à partir d'une forme contractée de ce message M obtenue au niveau du dispositif de saisie des données (4) ou au niveau des circuits de traitement (6), ou par tout autre dispositif intermédiaire approprié connu en soi et non représenté.

Cette signature SG est calculée par les circuits de traitement (6) à partir du programme P de calcul de signature et de la clé secrète S pré-enregistrés dans les zones (5a) et (5b) de la mémoire (5), respectivement. Il est important de noter que le programme P d'élaboration de signature SG peut être quelconque à la seule condition qu'il prenne en compte l'intégralité du contenu du message pour être certain que toute modification de son contenu, si mineure soit-elle, entraîne automatiquement une modification de la valeur de la signature associée au message. Du fait que le programme P prend en compte la clé secrète S, inconnue de l'émetteur, il est impossible à ce dernier de prédéterminer à l'avance la signature SG du message M qu'il désire transmettre.

Dans une trosième phase, la signature SG ainsi calculée est associée au message M et à l'identification I au niveau de l'ensemble des circuits (7) et cet ensemble subit éventuellement des modifications pour le rendre inintélligible avant son transfert vers le dispositif récepteur (3) par la voie de transmission (2).

Le message signé (M, I, SG) est reçu par l'ensemble des circuits (10) du dispositif récepteur (3). Ces circuits

(10) ont essentiellement pour fonction de restituer le message d'origine M avec sa signature SG et son identification I au niveau par exemple du dispositif de visualisation (11). Simultanément à cet affichage, qui n'est pas obligatoire, le message M, son identification I et sa signature SG peuvent être automatiquement imprimés sur le support papier (13) par l'intermédiaire du dispositif d'entrée-sortie (12).

Ensuite, toute personne au niveau du dispositif récepteur (3) peut prendre connaissance du message signé reçu du dispositif émetteur (1). Toutefois, si la personne au niveau du dispositif récepteur (3) considère que le message lui est addressé (tout simplement parce que son nom figure dans le message), elle peut s'assurer conformément à l'invention, de l'authenticité de la signature SG du message pour identifier son origine. Il suffit pour cela que cette personne ait en sa possession la carte de contrôle (3b) qui peut être à la disposition de plusieurs personnes.

Dans une première phase, la personne précitée ou récepteur doit accoupler la carte de contrôle (3b) au dispositif récepteur (3) pour initialiser le processus d'authentification de la signature SG du message M reçu.

Dans une seconde phase, le procédé d'authentification de la signature SG du message M reçu consiste tout d'abord à calculer la clé secrète S de l'émetteur du message, puis à recalculer la signature SG de ce message au niveau du dispositif récepteur (3), à partir des informations pré-enregistrées dans la carte de contrôle (3b). Pour cela, le récepteur, en supposant que le message est transcrit sur le support papier (13) précité, réintroduit le texte du message ainsi que son identification I dans le dispositif récepteur (3) par l'intermédiaire du dispositif

d'entrée-sortie (12). L'identification I et le message initial ou sa forme contractée sont transmis par les bornes d'entrée (21) aux circuits de traitement (15) de la carte de contrôle (3b) accouplée à l'appareil récepteur (3).

Pour calculer la clé secrète S de l'émetteur du message, les circuits de traitement (15) déroulent le programme P' enregistré dans la zone (14c) de la mémoire (14), ce programme prenant en compte l'identification I du message. Plus précisément, les n paramètres représentatifs de cette identification I sont utilisés comme n adresses identifiant n clés élémentaires parmi m clés élémentaires (m n) pré-enregistrées dans la zone secrète (14a) de la mémoire (14). Le programme P' va donc rechercher les n clés élémentaires adressées et reconstituer la clé secrète de l'émetteur du message en combinant ces n clés élémentaires. Bien entendu, cette clé secrète S ainsi déterminée doit être identique à la clé secrète pré-enregistrée dans la carte de signature (1b) attribuée à l'émetteur du message.

Ensuite, les circuits de traitement (15) recalculent automatiquement la signature SG du message fourni par le récepteur. Pour cela, les circuits de traitement (15) déroulent le programme P de calcul de signature pré-enregistré dans la zone (14b) de la mémoire (14). Ce programme P est strictement identique au programme P pré-enregistré dans la zone (5b) de la mémoire (5) de la carte signature (1b) accouplée au dispositif émetteur (1) au cours de la transmission du message M. Ce programme P prend en compte le contenu du message M et la clé secrète S telle que précédemment déterminée par le programme P'.

Dans une troisième phase, la signature SG recalculée par les circuits de traitement (15) est envoyée à une entrée

du dispositif comparateur (16). L'autre entrée du dispositif comparateur (16) reçoit, par l'intermédiaire des bornes d'entrée (24), la signature SG fournie par le récepteur par l'intermédiaire du dispositif d'entrée-sortie (12). Le dispositif comparateur (16) compare ces deux signatures et transmet par l'intermédiaire des bornes de sortie (26) un signal d'exitation à destination de l'élément témoin (17). Cette excitation intervient par exemple uniquement dans le cas où les deux signatures correspondent exactement.

Dans ces conditions le récepteur est informé uniquement du résultat de la comparaison vrai ou différent de la signature donnée par le récepteur et de la signature recalculée automatiquement par le dispositif récepteur (3).

Ainsi le dispositif récepteur (3) est en mesure de détecter toute modification au niveau du message et/ou de son identité et/ou de sa signature, sans dévoiler qu'elle aurait été la valeur de la signature correspondant à un message modifié. Dans ces conditions, toute fraude devient impossible et le récepteur d'un message a la possibilité de déterminer avec exactitude la provenance du message reçu.

Bien évidemment, un tel procédé d'identification nécessite une certaine conformité entre la carte de signature (1b) côté émission et la carte de contrôle (3b) côté réception, ces deux supports devant contenir des informations communes. Etant donné le caractère inviolable de ces supports, c'est au niveau de leur fabrication ou de leur première attribution à une personne ou groupe de personnes que ces problèmes sont réglés.

Par mesure de sécurité, il est également avantageux de prévoir au niveau de l'appareil récepteur (3) un compteur

d'usage (non représenté) qui limite le nombre d'authentifications possibles par la carte de contrôle (3b). Une telle limitation permet d'éviter une recherche par effet exhaustif susceptible de permettre de retrouver la clé secrète S attribuée à une personne.

REVENDICATIONS :

1. Procédé pour authentifier la signature d'un message signé reçu par un appareil récepteur (3) et transmis à partir d'un appareil émetteur (1) par une voie de transmission quelconque (2), la signature (SG) d'un message (M) étant élaborée automatiquement au niveau de l'appareil émetteur (1) à partir d'un programme (P) de calcul de signature faisant au moins appel au contenu du message (M) à transmettre et à un paramètre ou clé secrète (S) inconnue de la personne ou émetteur du message (M), caractérisé en ce qu'il consiste, pour vérifier l'authenticité de la signature (SG) d'un message (M) reçu par l'appareil récepteur (3) :

- à recalculer automatiquement la signature (SG) du message reçu (M) à partir d'au moins le même programme (P) précité prenant en compte le contenu du message (M) reçu et la même clé secrète (S) précitée également inconnue de la personne ou récepteur du message,

- à comparer automatiquement la signature (SG) du message reçu et la signature (SG) recalculée au niveau de l'appareil récepteur (3),

- à indiquer seulement au récepteur du message, le résultat égal ou différent de la comparaison précédente tout en interdisant au récepteur du message la possibilité de pouvoir prendre connaissance de la valeur de la signature recalculée.

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste :

- au niveau de l'appareil émetteur (1) : à autoriser plusieurs personnes à émettre des messages signés avec

élaboration automatique de la signature, chaque personne ayant d'une part une clé secrète (S) propre inconnue de la personne, et d'autre part une identité I non secrète transmise avec le message (M), et

- au niveau de l'appareil récepteur (3) : avant de recalculer la signature (SG) du message (M) reçu, à déterminer automatiquement la clé secrète (S) de l'émetteur du message (M) à partir de l'identité I de l'émetteur transmise avec le message (M).

3. Procédé selon la revendication 1 ou 2, caractérisé en ce qu'il consiste à subdiviser la clé secrète (S) de chaque personne émettrice d'un message (M) en n clés élémentaires secrètes choisies parmi m clés élémentaires secrètes regroupées dans une zone mémoire secrète (14a) de l'appareil récepteur (3), et à identifier chaque personne émettrice par n paramètres représentatifs des adresses de n clés élémentaires dans la zone mémoire secrète (14a), ces n paramètres ou identification I étant transmis avec le message (M) pour permettre à l'appareil récepteur (3) de calculer automatiquement et secrètement, au moyen d'un programme P', la clé secrète (S) de la personne émettrice avant de recalculer la signature (SG) du message (M) reçu.

4. Dispositif pour la mise en oeuvre du procédé tel que défini selon l'une des revendications précédentes, du type constitué par un appareil émetteur (1) relié par une voie de transmission quelconque (2) à un appareil récepteur (3), l'appareil émetteur (1) comprenant au moins un dispositif de mémorisation (5) dans lequel sont au moins enregistrés un programme (P) de calcul de signature et un paramètre ou clé secrète (S) inconnue de l'émetteur du message, des circuits de traitement (6) pour élaborer automatiquement la signature (SG) d'un message (M) à partir du programme (P) précité qui prend en compte le

contenu du message (M) et la clé secrète (S) précitée, caractérisé en ce que l'appareil récepteur (3) comprend au moins :

- un dispositif de mémorisation (14) dans lequel sont au moins enregistrés le programme (P) précité et la même clé secrète (S) précitée également inconnue du récepteur du message,

- des circuits de traitement (15) pour recalculer la signature (SG) d'un message reçu à partir du contenu du message, du programme (P) et de la clé secrète (S) précités,

- un dispositif de comparaison (16) dont une première entrée reçoit de l'extérieur la signature (SG) du message (M) reçu et dont la seconde entrée reçoit la signature recalculée précitée, et

- un dispositif témoin (16) à au moins deux états stables indiquant respectivement les résultats vrai ou différent de la comparaison précitée, l'entrée du dispositif témoin (16) étant reliée à la sortie du dispositif de comparaison (15).

5. Dispositif selon la revendication 4, caractérisé en ce que le dispositif de mémorisation (14) de l'appareil récepteur (3) contient une première zone secrète (14a) dans laquelle sont pré-enregistrés les m clés élémentaires précitées, et une deuxième zone (14c) dans laquelle est pré-enregistré un second programme (P') de calcul de la clé secrète (S) de la personne émettrice d'un message à partir des n paramètres précités représentatifs des n clés élémentaires et transmis avec le message (M).

6. Dispositif selon la revendication 4 ou 5, caractérisé en ce que l'appareil émetteur (1) est composé de deux

parties : une partie fixe (1a) accessible à toute personne et qui est destinée à assurer la transmission d'un message (M), et un dispositif portatif (1b) ou carte de signature, personnelle à chaque personne et renfermant de façon inaccessible depuis l'extérieur la clé secrète (S) de la personne, les circuits de traitement (6) pour calculer la signature (SG) d'un message (M) à partir du contenu du message (M) et de la clé secrète (S), et de préférence le programme (P) d'élaboration automatique de cette signature (SG).

7. Dispositif selon la revendication 4 ou 5, caractérisé en ce que l'appareil récepteur (3) est composé de deux parties : une partie fixe (3a) accessible à toute personne susceptible de recevoir un message (M), et un dispositif portatif (3b) ou carte de contrôle à la disposition de plusieurs personnes et renfermant, de façon inaccessible depuis l'extérieur, le dispositif de mémorisation (14) précité, les circuits de traitement (15) précités et le circuit de comparaison (16) précité.

8. Dispositif selon la revendication 7, caractérisé en ce que la borne d'entrée du dispositif de comparaison (16) précité qui reçoit la signature recalculée (SG) précitée est inaccessible depuis l'extérieur.

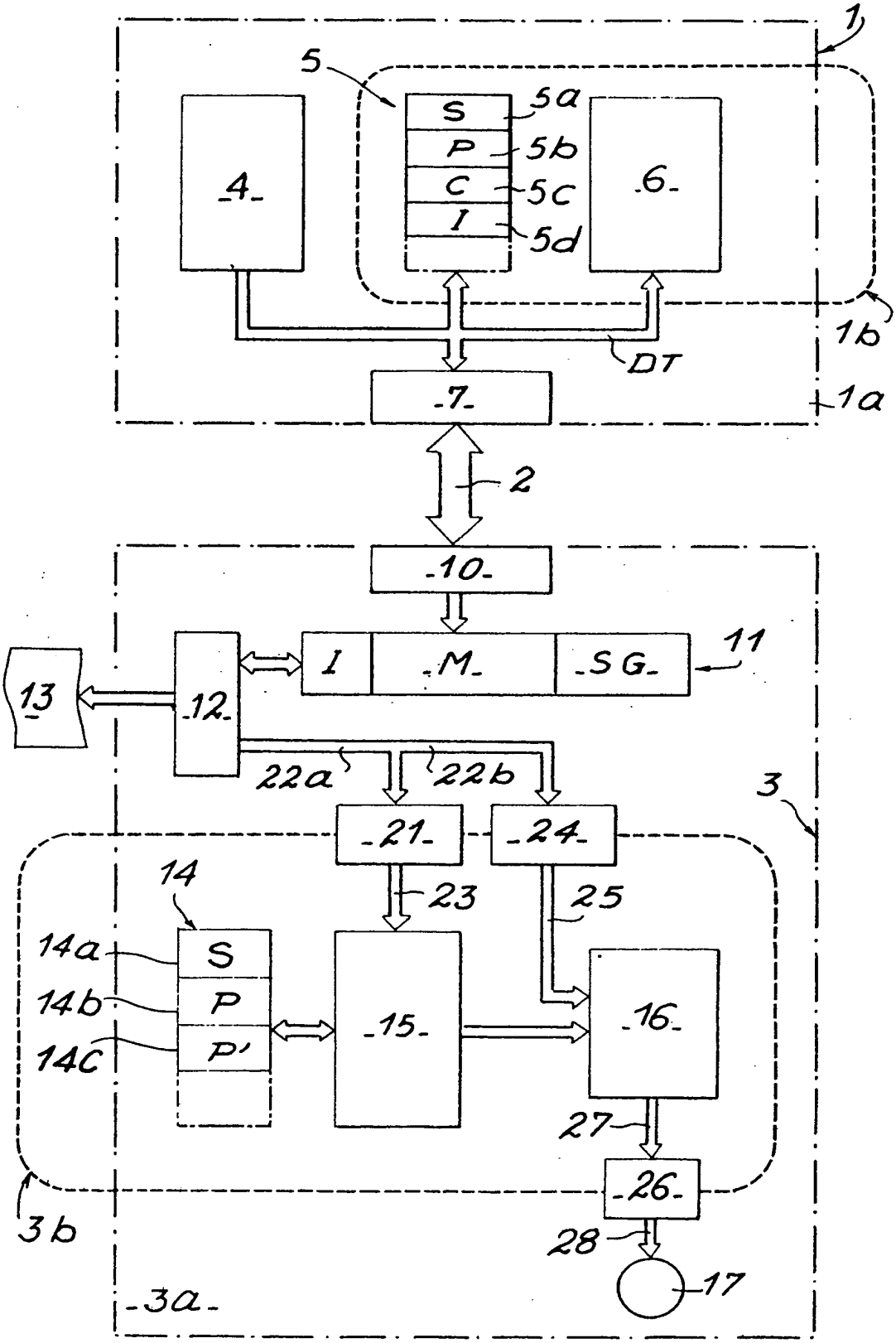
9. Dispositif selon la revendication 6, caractérisé en ce que la clé secrète (S) précitée et le programme de calcul (P) précité sont pré-enregistrés lors de fabrication de la carte de signature (1b).

10. Dispositif selon la revendication 7, caractérisé en ce que les informations contenues dans le dispositif de mémorisation (14) précité sont pré-enregistrées lors de la fabrication de la carte de contrôle (3b).

11. Dispositif selon la revendication 7, caractérisé en ce que l'élément témoin (17) précité est un témoin lumineux ou sonore.

12. Dispositif selon la revendication 11, caractérisé en ce que l'élément témoin (17) précité est porté par la partie fixe (3a) de l'appareil récepteur (3).

0077238


1
5
5a
S
5b
P
5c
C
5d
I
4
6
1b
DT
7
1a
2
10
11
I
M
SG
13
12
22a
22b
3
21
24
14
23
25
14a
S
14b
P
14c
P'
15
16
27
26
28
17
3b
3a

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande

EP 82 40 1752

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl. ³)
Y	PROCEEDINGS OF THE NATIONAL ELECTRONICS CONFERENCE, vol. 35, 1er octobre 1981, pages 296-301, Oak Brook, Ill. USA SMID: "Authentication using the Federal Data Encryption Standard" * Page 297, colonne de droite, lignes 34-38; colonne de droite, lignes 15-28 *	1	H 04 L 9/00
Y	EP-A-0 021 401 (IBM) * Page 5, lignes 24-30; page 6, ligne 21 - page 9, ligne 15 *	1	
A		2	
A	EP-A-0 035 448 (CII-HONEYWELL BULL) * Page 4, ligne 6 - page 5, ligne 27 *	6,7	DOMAINES TECHNIQUES RECHERCHES (Int. Cl. ³) H 04 L 9/00 H 04 L 9/02 G 07 F 7/10

Le présent rapport de recherche a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	14-01-1983	HOLPER G.E.E.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

OEB Form 1503. 03.82